JEDEDIAH WAKEFIELD (CSB No. 178058)
jwakefield@fenwick.com
TYLER G. NEWBY (CSB No. 205790)
tnewby@fenwick.com
KATHLEEN LU (CSB No. 267032)
klu@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350

Attorneys for Defendant
PATH, INC., a Delaware Corporation

Additional Counsel Listed on Signature Pages

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

APPLICATION DEVELOPER DEFENDANTS' REPLY BRIEF IN SUPPORT OF JOINT MOTION TO DISMISS CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Date: February 6, 2014
Time: 10:00 A.M.
Courtroom: 9
Judge: Hon. Jon S. Tigar

THIS DOCUMENT RELATES TO ALL CASES:

Opperman v. Path, Inc., No. 13-cv-00453-JST
Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST
Gutierrez v. Instagram, Inc., No. 12-cv-6550-JST
Espitia v. Hipster, Inc., No. 13-cv-0432-JST

TABLE OF CONTENTS

TABLE OF CONTENTS
Continued

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

TABLE OF AUTHORITIES
(Continued)

Page(s)

INTRODUCTION

The 422nd filing in this case does not say much more than the first. After numerous opportunities to refine their theory of the case, Plaintiffs' Opposition ("Opp.") simply rehashes the Consolidated Amended Complaint's ("CAC") allegations—though, notably, Plaintiffs have abandoned their RICO and vicarious liability claims. Opp. 36 n.22. As for their remaining 25 claims, Plaintiffs cite no authority demonstrating that the CAC includes any viable claims for relief. Nor do Plaintiffs offer any additional facts that could be pleaded to cure the CAC's deficiencies. Instead, Plaintiffs' recurring response to the majority of the App Defendants' arguments in their Joint Motion to Dismiss ("Motion") is that they need discovery. Rule 12, however, tests the sufficiency of the *allegations*, not Plaintiffs' hope to find facts to prove them. The allegations here fall short.

Plaintiffs' Opposition sets forth no viable Article III argument. Each theory of "injury" that Plaintiffs advance has been rejected by courts considering similar claims, and Plaintiffs did not even attempt to address Defendants' argument that lumping numerous unrelated Defendants together and generally attributing harm to the group is insufficient to establish harm "fairly traceable" to *each* individual Defendant.

Even if Plaintiffs could point to a concrete and particularized injury-in-fact, they fail to address adequately the shortcomings of their 25 claims for relief. In short, Plaintiffs conflate the elements of California Penal Code section 502 and the CFAA, misstate both, and end up stating a claim under neither—particularly because they do not, and cannot, allege any "unauthorized" access. Nor does the Opposition offer any argument regarding "loss," a necessary element of a CFAA claim. Plaintiffs argue that "copying" constitutes an "intercept" under ECPA and the state wiretap statutes and that it is an "interference" with property sufficient to constitute conversion. Plaintiffs, however, point to no case law supporting their "copying" theory and, in fact, case law is to the contrary. Nor do Plaintiffs cite any authority to support their argument that hypothetical disclosure of contacts to ISPs, cellular companies or Defendants' employees is a disclosure to the "public at large" for purposes of the invasion of privacy claim. And, they cite no authority supporting their argument that a *de minimis* loss of battery life or memory, such as they

allege here, supports a trespass to chattels claim. Indeed, relevant authority is to the contrary on all counts. Nor do Plaintiffs allege they used their contacts in commerce or suffered commercial damages, as necessary to support a misappropriation claim. Last, Plaintiffs concede that some apps obtained consent, but now argue that the consent was invalid. They point to no allegations, however, sufficient to vitiate consent and thus leave their new argument wholly unsupported by their old allegations.

Because the CAC's factual allegations neither establish injury to any Plaintiff nor satisfy the elements of the 25 causes of action, it should be dismissed. Plaintiffs cannot save any claims by yet another amendment, and the CAC should be dismissed with prejudice.

I. PLAINTIFFS CANNOT ESTABLISH ARTICLE III STANDING

A. Plaintiffs Have Failed to Plead any Injury-in-Fact

Rather than address their failure to allege "concrete" and "particularized" injury as required to establish Article III standing, Plaintiffs accuse the App Defendants of failing to assume that the allegations of the complaint are true.[1] *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000); Opp. at 6. Not so. Even assuming the truth of the allegations, as the App Defendants do throughout their Motion, Plaintiffs have failed to allege any "concrete" or "particularized" injury.

First, Plaintiffs' insistence that they have standing because their contacts have market value fails because Plaintiffs have not alleged, and do not address in their Opposition, how Defendants' actions have *diminished* that value or otherwise caused harm.[2] Plaintiffs do not argue that the App Defendants made the information unsuitable for sale or interfered with Plaintiffs' use of their contacts. Nor do they claim that Defendants took exclusive copies of contacts off Plaintiffs' devices. Thus, as several courts have held in nearly identical situations, there is no injury for purposes of standing. *See In re Google, Inc. Privacy Policy Litig.*, No. C-

[1] Plaintiffs may be confusing the App Defendants with Apple, which included a partial Article III challenge in its motion to dismiss the CAC. The App Defendants' Article III challenge is purely facial.

[2] Plaintiffs' claim that the range of value is as high as $17,000 per address book strains credulity, but that does not affect the legal analysis at this stage of the litigation.

12-1382-PSG, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013) ("[A] plaintiff *must* allege how the defendant's use of the information *deprived the plaintiff of the information's economic value*.") (emphasis added); *In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264 JSW, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) (allegations that defendant's collection of personally identifiable information ("PII") diminished its market value were insufficient to show injury because plaintiffs did not allege they had tried and failed to sell their PII or were foreclosed from doing so in the future). Nor have Plaintiffs alleged that Defendants somehow interfered with Plaintiffs' own use of their contacts. They cannot, because—unlike the "theft" of a physical address book (Opp. at 10)—the digital contacts on Plaintiffs' iDevices remain unaltered and available for Plaintiffs' use.

Plaintiffs try to distinguish the numerous cases rejecting identical theories of standing on the ground that, unlike this case, those cases did not involve "property."[3] Opp. at 10 (arguing contacts "are clearly property belonging to the Plaintiffs"). Plaintiffs, however, offered no authority supporting their contention that their contacts, which are digital compilations of other people's contact information, constitute "property." Plaintiffs' conclusory legal assertion, untethered to any cognizable theory that their compilation of contact information is somehow protected by property law, should be rejected.

Even if Plaintiffs could assert a property interest in their contacts, Plaintiffs' purported factual distinction makes no difference. The relevant Article III issue is not whether electronic information is "property." In the cited cases, the courts assumed that the electronic information at issue was the plaintiff's "property" but still found no standing. The key is *injury*—"property" or not, uninjured plaintiffs have no standing. Plaintiffs fail to plead injury for Article III purposes because they do not allege that Defendants' deprived them of the information's alleged economic value. *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5.

Plaintiffs next argue that "[*a*]*ny* alleged trespass upon property or invasion of privacy triggers constitutional standing." Opp. at 9. This unsupported argument directly contradicts both

[3] Plaintiffs characterize the information at issue in those cases as "automatically-generated computer data sets" such as an individual's Internet browsing and search history, personal identifiers, and GPS records of a person's movements which, they contend, are not "property."

California law regarding trespass to chattels and California and U.S. Supreme Court precedent requiring plaintiffs to have suffered an injury in fact. *See, e.g.*, *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1351 (2003) (to state a claim for common law trespass to a computer, plaintiffs must allege demonstrable damage to the computer or that plaintiffs were prevented from using the computer); *Friends of the Earth*, 528 U.S. at 180-81; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). In *Intel Corp.*, the California Supreme Court explained that "under modern California and broader American law," "while a harmless use or touching of personal property may be a technical trespass, such an interference (not amounting to dispossession) is not *actionable* . . . without a showing of harm." *Id.* at 1351 (internal citation omitted; emphasis in original).

In an attempt to avoid *Intel's* harm requirement, Plaintiffs cite only a law review article that actually supports Defendants' position. While the article mentions standing in trespass on property cases in the context of an English case from 1348 and two legal treatises from the 1920s, it recognizes the modern standard that "plaintiffs no longer have standing to bring claims based solely on the violation of their personal rights; they must demonstrate that some factual harm resulted from the violation." F. Andrew Hessick, *Standing, Injury in Fact, and Private Rights*, 93 CORNELL L. REV. 275, 277 (2008).

Plaintiffs' allegations regarding use of "battery life, energy, cellular time, storage, space, and bandwidth" similarly fail to establish standing. Plaintiffs simply ignore numerous cases rejecting identical claims (*see* Motion at 9-10), including the court's decision in *Hernandez v. Path, Inc.*, No. 12-CV-1515 YGR, 2012 WL 5194120, at *4 (N.D. Cal. Oct. 19, 2012) (rejecting identical allegations as "*de minimus*" (sic)); *see also Caldwell v. Caldwell*, 545 F.3d 1126, 1134 (9th Cir. 2008) (concurrence) (*de minimis* injury does not support standing).

Finally, Plaintiffs' allegation that they "will incur" costs simply to remove the apps from their devices is both insufficient and factually implausible. Plaintiffs do not allege that any of them has been "forced" to hire an expert to remove any app, notwithstanding that they allege they learned about the challenged conduct nearly two years ago. *See* CAC ¶ 48 (defining the "Malware Subclass" as those purchasing the apps "before February 2012"); ¶ 131 (the alleged "unauthorized transmissions . . . continued until at least early February 2012"); ¶ 267 (Path's

alleged actions "re-occurred …up through February 6, 2012"). Plaintiffs' reliance on Judge Gonzalez-Rogers' opinion is completely misplaced. Her opinion was based on an express allegation in *Hernandez* that an expert was necessary to remove "tracking code" that allegedly had been embedded in digital media files on the plaintiff's phone. *Hernandez*, 2012 WL 5194120, at *2. Plaintiffs have since dropped that allegation, which was separate from the contacts allegations at issue here, and do not assert it against any of the App Defendants. There are no factual allegations in the CAC supporting an argument that Plaintiffs must hire experts simply to delete Defendants' apps.

Even if it were not facially implausible, a conclusion that Plaintiffs' "expert removal" allegations here establish Article III standing would contradict recent United States Supreme Court authority. *See Clapper v. Amnesty Int'l USA*, __ U.S. __, 133 S. Ct. 1138, at *1154 (2013). In *Clapper*, the Supreme Court held that costs incurred to avoid allegedly illegal surveillance by the United States did not establish Article III standing because the plaintiffs failed to establish "a threat of certainly impending interception." *Id*. Similarly, Plaintiffs cannot establish standing based on the costs they claim they will incur to remove the apps from their devices because they do not allege that Defendants' purported wrongful accessing of their contacts is ongoing or "certainly impending." Absent an allegation of "certainly impending" harm underlying the alleged cost of removing the apps from their devices, any such costs that have or will be incurred would be "simply the product of [Plaintiffs'] fear" and "fear is insufficient to create standing." *Clapper*, 133 S. Ct. at *1154; *see also United States v. Kriesel*, 720 F.3d 1137, 1147 (9th Cir. 2013) ("[I]f the plaintiffs in *Clapper* lacked standing to complain of injury that was only speculative, then Kriesel's demand for return of property lacks merit when founded upon similar speculative concerns about possible future government conduct.").

Separate from whether Plaintiffs have identified some injury-in-fact, they failed to address traceability at all. Instead, Plaintiffs continually refer to the alleged harm as attributable to Defendants collectively. For the reasons stated in the App Developer's opening brief, this is

insufficient to establish Article III standing. Dkt. 396 at 13-14.[4] On this basis alone, Plaintiffs have failed to establish standing.

B. Plaintiffs' Request for Injunctive Relief Does not Establish Standing

Plaintiffs next argue that their request for injunctive relief establishes standing even absent injury-in-fact. Opp. at 8. Plaintiffs are wrong. A plaintiff must demonstrate "that he is realistically threatened by a repetition of [the unlawful conduct]" to have standing to assert a claim for prospective injunctive relief. *City of Los Angeles v. Lyons*, 461 U.S. 95, 109 (1983). Plaintiffs, however, have pleaded that Defendants *ceased* the challenged conduct in February 2012. *See, e.g.*, CAC ¶¶ 48, 131, 267, 269, 308, 323, 353, 359, 381, 401 (alleging various defendants began expressly requesting permission to access and transmit contacts beginning in February 2012). Accordingly, Plaintiffs have failed to allege any realistic threat of repetition.

Plaintiffs' own authority concedes that "recurring injury" is a prerequisite to injunctive relief. *See* Opp. at 8 (citing *Nicacio v. U.S. I.N.S.*, 797 F.2d 700 (9th Cir. 1985) ("recurring injury" establishes standing to seek injunctive relief)). As described, even the purported "violations" Plaintiffs complain of have not actually "injured" them, and there is no allegation that such "violations" will occur again. Because they have alleged neither ongoing violations nor recurring harm resulting from those violations, Plaintiffs cannot rely on their request for injunctive relief to supply Article III standing. *Lyons*, 461 U.S. at 109; *Marcavage v. City of New York*, 689 F.3d 98, 103 (9th Cir. 2012) (no standing in light of plaintiffs' failure to "demonstrate[] a certainly impending future injury").

C. Plaintiffs' Statutory Claims Fail to Establish Standing

Plaintiffs' argument that allegations of statutory violations are sufficient to establish standing fails. Opp. at 8-9. The mere assertion of a statutory violation does not always confer Article III standing. *See Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997) (holding "it is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing"); *Summers v. Earth Island Inst.*, 555 U.S.

[4] Plaintiffs do not dispute that their allegations against Defendants Instagram and Path are insufficient to establish standing based on the alleged diminution of their iDevices' value. *See* Motion at 10-11.

488, 497 (2009) (noting that "injury in fact is a hard floor of Article III jurisdiction that cannot be removed by statute"); *Fulfillment Servs. v. UPS*, 528 F.3d 614, 619 (9th Cir. 2008) ("[N]ot all statutes endow rights on a given plaintiff, the infringement of which is sufficient to support standing."); *Robins v. Spokeo, Inc.*, No. CV10-5306 ODW (AGRx), 2011 WL 597867, at *1 (C.D. Cal. Jan. 27, 2011) (noting that "even when asserting a statutory violation, the plaintiff must allege 'the Article III minima of injury-in-fact'") (citation omitted).[5] Moreover, Plaintiffs fail to identify which, if any, of their claims are based on a statute that creates a legal right sufficient to satisfy the injury-in-fact requirement. Even if Plaintiffs were able to identify such a statute, because all of Plaintiffs' statutory claims fail, those claims fail to confer Article III standing.[6]

II. EACH CLAIM OF THE CAC SHOULD BE DISMISSED UNDER RULE 12(b)(6)

A. Plaintiffs' UCL Claim Should Be Dismissed

1. Plaintiffs Lack UCL Standing

Economic injury and causation are strict requirements under the UCL.[7] Cal. Bus. & Prof. Code § 17204. Plaintiffs contend they have UCL standing because they have an unsubstantiated "property interest" in their mobile contacts. Opp. 14-15. But even assuming a property interest to begin with, such an interest alone cannot establish economic injury.[8] To have standing, Plaintiffs must allege the App Defendants' actions caused them to suffer an economic loss. *See*

[5] Plaintiffs' reliance on *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2007) is misplaced, as *Edwards* involved a statute not at issue here.

[6] In the event the Court concludes Plaintiffs stated a claim for any statutory violation, and that the statutory violation itself confers Article III standing, Plaintiffs would be able to proceed only on that theory, and not on other statutory and common law theories.

[7] The UCL requires a plaintiff to "(1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., *economic injury*, and (2) show that that economic injury was the result of, i.e., *caused by*, the unfair business practice or false advertising that is the gravamen of the claim." *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 322 (2011) (emphasis in original).

[8] Plaintiffs have no authority for this proposition. The cases cited by Plaintiffs do not concern the UCL. *See Rakas v. Illinois*, 439 U.S. 128, 150 (1978) (affirming judgment of conviction because the Illinois courts were "correct in concluding that it was unnecessary to decide whether the search of the car might have violated the rights secured to someone else by the Fourth and Fourteenth Amendments to the United States Constitution"); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1073 (N.D. Cal. 2000) (enjoining Bidder's Edge from accessing eBay's computer systems or networks for the purpose of copying any part of eBay's auction database).

Folgelstrom v. Lamps Plus Inc., 195 Cal. App. 4th 986, 994 (2011) ("[E]ven if plaintiff had an intellectual property interest in his address, he does not explain how that interest has been economically diminished. . . . The fact that the address had value to Lamps Plus, such that the retailer paid Experian a license fee for its use, does not mean that its value to plaintiff was diminished in any way."). Plaintiffs have made no such allegation.

Although Plaintiffs again rely on their "diminished economic value" theory, that theory cannot save their UCL claim because they do not claim to have lost access to or use of their contacts. *See Yunker v. Pandora Media, Inc.*, No. 11–CV–03113 JSW, 2013 WL 1282980, at *11 (N.D. Cal. Mar. 26, 2013) (no standing under the UCL where plaintiff failed to show information "cease[d] to belong to him or pass[ed] beyond his control") (citing *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 863 (N.D. Cal. 2011)).[9]

This leaves Plaintiffs with their disclosure theory, but disclosure of personal information alone is not a cognizable injury under the UCL. *See, e.g., In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011); *Thompson v. Home Depot, Inc.*, No. 07-cv-1058, 2007 WL 2746603, *3 (S.D. Cal. Sept. 18, 2007). Plaintiffs' attempt to distinguish their contacts from the personal information that was at issue in the above cases fails. *See* Opp. 14. As with other collections of names, addresses, financial data, and emails, Plaintiffs' allegations that the collection of their contacts, without more, caused them injury are too indefinite to meet the heightened degree of injury required by the UCL. *See Claridge*, 785 F. Supp. 2d at 863.

Finally, Plaintiffs' attempt to assert California claims against App Defendants Foursquare, Kik, Rovio, ZeptoLab (none of which are headquartered in California),[10] and

[9] Plaintiffs ask this Court to ignore *Claridge* because it cites to authority disapproved by the California Supreme Court in *Kwikset*. Opp. 14. However, nothing in *Kwikset* rejects the principle that under the UCL, a plaintiff must actually sustain an economic loss of some type. *Kwikset* simply disapproved the proposition that a plaintiff must show a *corresponding gain* by the defendant to have UCL standing. *Kwikset*, 51 Cal. 4th at 335.

[10] The Opposition fails to justify the application of California statutory and common law causes of action to these Defendants, none of which are alleged to have conducted any relevant business operations in California. The Opposition argues that these Defendants are subject to California law because of their affiliation with Apple as their "California agent," but the Opposition later abandons its "agency" theory. Opp. 36, n. 22. Apple's alleged California conduct thus cannot be attributed to non-California defendants, *see* Motion at 49-50, and no California-based conduct is otherwise alleged.

Instagram[11] fails. California Plaintiff Haig Arabian withdrew his claims after Defendants filed this Motion, and the only remaining California Plaintiff (Lauren Carter) downloaded only Path's app. *See* CAC ¶¶ 16-31; Dkt. No. 426. Because the non-California Plaintiffs have not alleged that they were injured in California, that any misconduct occurred here, or that any other basis exists to apply California law to their claims against Foursquare, Kik, Rovio, ZeptoLab, and Instagram, their California-law claims against those Defendants should be dismissed. *See Gross*, 2012 WL 3116158, at *6.

2. Plaintiffs Have not Plausibly Alleged any Actionable Misconduct

Plaintiffs' UCL claim should also be dismissed because Plaintiffs have not plausibly alleged any "unlawful," "unfair," or "fraudulent" business practices, as required to state a UCL claim. Cal. Bus. & Prof. Code § 17200. Plaintiffs' only argument in support of their "unlawful" allegations is that it is not possible for all of their statutory claims to fail. But Plaintiffs do not deny that if the Court grants the App Defendants' motion to dismiss all of Plaintiffs' statutory claims, then Plaintiffs' claims under the "unlawful" prong of the UCL must also be dismissed.

Plaintiffs do not even bother to argue that their allegations of "fraudulent" conduct meet the heightened pleading requirements of Fed. R. Civ. P. 9(b). Of course, Plaintiffs would be hard-pressed to make this argument. By lumping all of the App Defendants together in the CAC, Plaintiffs fall short of the requirement that each defendant be informed of its allegedly fraudulent conduct. *See Swartz v. KPMG LLP*, 476 F.3d 756, 764-65 (9th Cir. 2007).

Finally, Plaintiffs maintain that whether the App Defendants engaged in "unfair" conduct is a "merits" question that cannot be made in the abstract on a motion to dismiss. However, courts routinely dismiss UCL claims at the pleading stage where, as here, "unfair" conduct is not plausibly alleged. *See, e.g.*, *Eghtesadi v. Wells Fargo Bank, N.A.*, No. 12-CV-1978-GPC-JMA, 2013 WL 1498999, at *11-12 (S.D. Cal. Apr. 11, 2013); *Fabozzi v. StubHub, Inc.*, No. C-11-4385

[11] Plaintiffs' allegation that Instagram is headquartered in California is, on its own, insufficient to rebut the presumption against the extraterritorial application of California statutes. *See Gross v. Symantec Corp., No. 12-C-00154-CRB*, 2012 WL 3116158, at *7-86 (N.D. Cal. July 31, 2012); *see also Tidenberg v. Bidz.com, Inc.*, No. 08-CV-5553-PSG, 2009 WL 605249, at *4–5 (C.D. Cal. Mar. 4, 2009) (rejecting argument that court can presume unlawful conduct emanated from California merely because defendant is headquartered there).

EMC, 2012 WL 506330, at *7-8 (N.D. Cal. Feb. 15, 2012); *Sarbaz v. Wachovia Bank*, No. C 10-03462 CRB, 2011 WL 830236, at *4 (N.D. Cal. Mar. 3, 2011). Here, the App Defendants allegedly accessed Plaintiffs' contacts "for a reason" (Opp. 15) – *to provide Plaintiffs with the social networking features of the apps they installed*. That is not unfair, and Plaintiffs' UCL claim should be dismissed in its entirety.

B. Plaintiffs Fail to State a Claim Under California Penal Code Section 502

Plaintiffs misunderstand section 502(c), which is intended to deter criminal hacking. *See Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29, 34 (2007) (defining access under section 502(c) in terms of hacking).[12] Ample case law holds that a defendant violates section 502(c) only by circumventing technical barriers, or otherwise engaging in hacking. *See In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715-16 (N.D. Cal. 2011); *In re iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at *12-13 (N.D. Cal. Sept. 20, 2011) ("*iPhone I*"); *Chrisman*, 155 Cal. App. 4th at 34; *Facebook, Inc. v. Power Ventures, Inc.*, No. C 08-05780 JW, 2010 WL 3291750, at *7-8 (N.D. Cal. July 20, 2010). Indeed, *In re iPhone I* involved nearly identical facts and claims, including allegations that mobile applications improperly accessed areas of Plaintiffs' devices without their consent, and squarely applies to this case. Similarly, *Chrisman* involved a closed company computer network, and *In re Facebook* and *Power Ventures* both involved password-enabled websites. Plaintiffs argue that these cases are inapplicable because they involved access of "open websites" and "open networks," but as described above, this purported distinction does not exist.[13]

Plaintiffs contend that section 502 does not *always* require circumvention of a technical barrier, citing *Weingand v. Harland Fin. Solutions, Inc.*, No. C-11-3109 EMC, 2012 WL 2327660 *1, 5 (N.D. Cal. June 19, 2012), and *Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087,

[12] Plaintiffs create a straw man by attempting to distinguish *In re Apple & ATTM Antitrust Litig.*, 596 F. Supp. 2d 1288 (N.D. Cal. 2008), a case Defendants did not cite in seeking dismissal of the section 502 claims.

[13] Contrary to Plaintiffs' assertion, Judge Gonzalez-Rogers did not hold that use of address book contacts created a question of fact preventing dismissal in all claims alleging § 502. Instead, the decision was expressly limited to the facts of that case, due to the "current limited briefing" regarding whether the allegations fell outside of § 502. *Hernandez*, 2012 WL 5194120 at *4.

1091 (N.D. Cal. 2007). Opp. at 19-20. Critically, however, the defendants in *Weingand* and *Facebook* had no authority of any kind to access the systems at issue—and therefore the court did not need evidence that defendants overcame technical barriers in order to find they acted without permission. *See* Motion at 20-21. That is simply not the case here.

Indeed, Plaintiffs offer no plausible standard for determining when an act is done "without permission," other than their own subjective belief that the apps they downloaded *should* not access their contacts. This expansive reading would permit iDevice users to "invent their own criminal law" based on their subjective expectations of the permission they grant when downloading an App—the very problem Plaintiffs claim led the court in *Power Ventures* to adopt the technical barriers requirement. *See* Opp. at 19-20.[14]

Finally, Plaintiffs argue, without support, that any code that "transmits information" constitutes a "contaminant" under the statute. Opp. at 21. This expansive reading ignores the plain language of the statute: a "contaminant" must "usurp the normal operation" of the computer or system. *See* Cal. Penal Code § 502(c)(10) (defining contaminant); *see also In re Facebook Privacy*, 791 F. Supp. 2d at 716 n.11 (dismissing plaintiffs § 502(c)(8) claims where they failed to allege the technology usurped the normal operation of their computer). A "contaminant" is not simply a set of instructions, but instead is a set of instructions that negatively interferes with the normal operation of a computer or system. Plaintiffs have not alleged such interference.[15]

[14] Plaintiffs argue, for the first time, that the App Defendants overcame technical barriers. They assert that the technique of "sandboxing" uses technical barriers to prevent one App from accessing data from another. (Opp. at 20, n. 12.) Plaintiffs have never alleged that the App Developers accessed data *from one another*, but merely that they accessed the information from Plaintiffs. Further, this theoretical discussion of App design is contradicted by Plaintiffs' allegations that Apple, the designer of Plaintiffs' iDevices, teaches App Developers to access address book data. Accepting this as true, there is no plausible allegation in the CAC of any technological barriers to accessing such data.

[15] Plaintiffs describe the rule of lenity as applying to "those situations in which a reasonable doubt persists about a statute's intended scope . . .". At best, Plaintiffs' argument is that overcoming technical barriers may not always be necessary to impose criminal liability. Opp. at 20. Thus, Plaintiffs themselves doubt the scope of the statute, affirming the lenity doctrine's applicability to this case. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) ("[i]t is well established that 'ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.'") (citation omitted); *Power Ventures*, 2010 WL 3291750, at *11-12 (holding the rule of lenity required a showing that the defendant overcame technical barriers in accessing a website to find he acted "without permission" under § 502).

Count X of the CAC should therefore be dismissed with prejudice.

C. Plaintiffs Fail to State a Claim Under the CFAA

1. Plaintiffs Fail to Allege Damage or Loss Under the CFAA

Plaintiffs allege that Defendants' conduct has caused aggregate "loss" in excess of $5,000, as subsection (c)(4)(A)(i)(I) requires to state a claim. CAC ¶ 572; 18 U.S.C. §1030(c)(4)(A)(i)(I). Application of subsection I, however, is restricted to the traditional computer 'hacker' scenario where the hacker deletes information, infects computers, or crashes networks." *AtPac v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010).[16] "Loss" under that subdivision is therefore defined as reasonable costs *actually incurred* as a result of defendant's conduct. *Id.*, § 1030(e)(11) (emphasis added). To satisfy the damage requirement, then, Plaintiffs must allege impairment to the integrity or availability of data, a program, a system, or information, of at least $5,000 in value. *Id.*, § 1030(e)(8), (g).

In their Opposition, however, Plaintiffs do nothing more than repeat their vague, rote statements of harm by virtue of alleged "de-privatization" of contacts; unspecified "loss in iDevice utility"; and speculative, indeterminate future expenses. Opp. at 22: 12-15. There is no allegation or argument that the iDevices were hacked or damaged in the aggregate amount of $5,000. *See, e.g.*, *Del Vecchio v. Amazon.com*, No. 11-366 RSL, 2012 WL 1997697, at *3-6 (W.D. Wash. June 1, 2012) (failure to allege facts showing devaluation of personal information or that plaintiffs discerned any difference in performance of computer when they visited defendant's website); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *10 (N.D. Cal. Mar. 26, 2013) (dismissing CFAA claim where insufficient facts alleged to reasonably infer that diminished memory storage would reach the $5,000 threshold, even if aggregated).[17] Plaintiffs' naked

[16] Noting that an aggregate loss claim "is grouped along with the harms of physical injury, threat to public health and safety, impairment of medical diagnosis or treatment, and damage to federal government computers that deal with national security and defense," and concluding that the definition of "loss" under subsection (I) has been narrowly interpreted "given the company that subsection (I) keeps." *AtPac*, 730 F. Supp. at 1185.

[17] *See also Capitol Audio Access, Inc. v. Umemoto*, No. 13-134, 2013 WL 5425324, F. Supp. 2d (E.D. Cal. Sept. 27, 2013) (failure to allege impairment to the integrity or availability of data, or a loss due to interruption of service, as required to state a CFAA claim); *Doyle v. Taylor*, No. 09-158, 2010 WL 2163521, at *2 (E.D. Wash. May 24, 2010) (where plaintiff alleged defendant accessed his USB thumb drive and retrieved a sealed document, "[p]laintiff would have to show

assertions fail to set forth "facts sufficient to demonstrate that a $5,000 loss *ha[s] actually occurred*," and thus are insufficient to state loss or damage under the CFAA. *Del Vecchio*, 2013 WL 1282980, at *4 (emphasis added); *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

2. Plaintiffs Fail to Allege Unauthorized Access or That Defendants Intentionally Caused Damage

Plaintiffs concede that they gave Defendants "permission to access their hardware" and "to install apps." Opp. at 18. This authorization is all that is required to defeat a claim of "without authorization" under §1030(a)(2)(C). *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009).

Plaintiffs also fail to allege that Defendants "exceed[ed] authorized access" under the CFAA for the reasons discussed in the App Defendants' Motion. *See also United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (noting CFAA's purpose is to "punish hacking – the circumvention of technological access barriers"). Plaintiffs have not plausibly alleged there were any technical restrictions placed on the App Defendants' access to their contacts. To the contrary, the CAC expressly alleges that Apple's iOS operating system enabled access. CAC ¶ 213 (alleging "Apple's iOS Human Interface Guidelines manual teaches and suggests Program registrants design and build apps that: (a) directly and automatically access contact data"); Motion at 19.[18]

Plaintiffs' reliance on *Weingand* is misplaced. In *Weingand*, the cross-complaint specifically alleged that the permission was limited to accessing "personal files." *Weingand*, 2012 WL 2327660 at *2. Here, Plaintiffs do not specify the technical boundaries (if any) of the permission they gave to Defendants by virtue of downloading the apps. This omission is particularly glaring given Plaintiffs' separate allegation that Apple's guidelines expressly instructed Defendants on how to "access . . . and upload the mobile address book maintained on

---

that the thumb drive itself was somehow damaged or impaired by Defendant's act of accessing the drive"); *AtPac*, 730 F. Supp. 2d at 1185.

[18] Further, the CAC does not meet the CFAA's "without authorization" or "exceeds authorized access" prohibitions, because it merely alleges misuse of Plaintiffs' contacts. *See e.g.*, CAC at ¶ 573 (alleging Defendants' violated CFAA by transmitting their contacts); *Nosal*, 676 F.3d 863-64 (holding that CFAA does not prohibit the use of data accessed with authorization).

Apple iDevices." *See* CAC ¶¶ 190, 213. The CAC does not create a reasonable inference that Plaintiffs limited Defendants' authorization and that Defendants exceeded that limitation. Finally, Plaintiffs fail to allege that Defendants intended to cause damage, as required under §1030(a)(5)(A), nor do they offer any response to Defendants' argument on this point.

D. Plaintiffs Fail to State Claims for Violation of the Electronic Communications Privacy Act or the California and Texas Wiretap Acts

Plaintiffs do not allege that any App Defendant "intercepted" any "transmission" of Plaintiff's contacts. Instead, Plaintiffs argue that a transmission occurs when an app "causes the iDevice to send information from the user's contacts from the iDevice's storage memory to processors and active memory being used by the app (referred to as an I/O operation)." Opp. at 23. But this is simply an allegation of copying data that was in storage. Plaintiffs do not allege that the contacts were being transmitted to or from the device when the apps allegedly copied them. Absent such an allegation, Plaintiffs have not alleged an "interception."

Controlling Ninth Circuit precedent forecloses Plaintiffs' argument that copying stored messages states a claim for violation of the Wiretap Act. *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077-78 (9th Cir. 2003). Courts applying *Theofel* have repeatedly rejected Plaintiff's copying theory. In *Bunnell v. Motion Picture Ass'n of Am.*, for example, the court held that accessing email stored on a server did not violate the Wiretap Act because the messages were in storage and, therefore, were not "intercepted." *See* 567 F. Supp. 2d 1148, 1154 (C.D. Cal. 2006) (holding that "the ordinary meaning of the word 'intercept'" requires an action that "halt[s] the transmission of the messages to their intended recipients"); *see also Garcia v. Haskett*, No. 05-3754 CW, 2006 WL 1821232 (N.D. Cal. June 30, 2006) (same, even though emails were unread); *Murray v. Fin. Visions, Inc.*, No. 07-2578-PHX-FJM, 2008 WL 4850328 (D. Ariz. Nov. 6, 2008) (same); *Exec. Sec. Mgmt., Inc. v. Dahl*, 830 F. Supp. 2d 883 (C.D. Cal. 2011) (same).[19]

[19] Similarly, in *United States v. Ropp*, the court dismissed a criminal wiretap indictment where the defendant had installed a keylogger on a victim's computer and used it to record the victim's keystrokes. 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004). The court held that the captured keystrokes were not "electronic communication" within the Wiretap Act because the internal communications on the computer were "not transmitted by a system that affects interstate or foreign commerce." *Id.*

Even the Seventh Circuit and Central District of Illinois cases Plaintiffs cite do not support their theory. *Shefts* and *Szymuszkiewicz* involved email auto-forwarding software that automatically sent the defendant every email the victim sent or received as the victim sent or received them. *Shefts v. Petrakis*, No. 10-cv-1104, 2012 WL 4049484, at *8 (C.D. Ill. Sept. 13, 2012)[20]; *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). Although those courts held the that the real-time email auto-forwarding processes alleged to have been used by the defendants in those cases satisfied the Wiretap Act's interception element, *Shefts* found that a defendant's copying of *stored* text messages from a Blackberry mobile device server through periodic synchronization was not an interception, because the messages were not copied simultaneously with their transmission to or from the victim. *Id.* at *8. Similarly, and fatally, Plaintiffs here allege only that Defendants accessed their contacts from local storage.

Finally, the App Defendants could not have "intercepted" any communications in violation of the Wiretap Act because, under Plaintiffs' theory, Defendants were both the senders and the recipients of the contacts. The Act expressly precludes a violation "where such person is a party to the communication." 18 U.S.C. § 2511(2)(d). In an effort to avoid this fatal flaw, Plaintiffs argue that the supposed communication "was between the storage memory and active application on the iDevice; it was not a communication to the App Defendants." Opp. at 25. Not only is this akin to saying that the device was talking to itself, but the argument ignores the CAC's allegation that the so-called communication between "storage memory and active application" was initiated by the App Defendants for the purpose of copying the contacts to the App Defendants' servers. Even assuming this constitutes a "communication," it was merely incidental to an alleged communication initiated by the App Defendants, who were parties to that communication. Accordingly, the claim fails.

E. Plaintiffs Fail to Plead a Common Law Privacy Claim

1. Plaintiffs Do not Allege a Disclosure to the Public at Large

Plaintiffs argue that they satisfy the "public disclosure" element by alleging that by uploading Plaintiffs' contacts to the App Defendants' servers, the App Defendants made the

[20] Plaintiffs incorrectly cite *Shefts* as a Central District of California case. Opp. at 25.

contacts "available" to the cellular and Internet service providers over whose networks the data travelled. Plaintiffs also argue that the App Defendants "disclosed" the contacts by making them available to their own employees, service providers or certain other App Defendants. Even assuming these allegations to be true, they do not allege the disclosure to the "the public in general" that is required to state a common law privacy claim. *See Porten v. Univ. of S.F.*, 64 Cal. App. 3d 825, 828 (1976); *see Johnson v. Sawyer*, 47 F.3d 716, 731 (5th Cir. 1995) (en banc) (under Texas law, information must be "communicated to the public at large"). Plaintiffs try to avoid this flaw by characterizing the issue as one of fact. But the sufficiency of public disclosure allegations is a legal question and is appropriately determined on the pleadings. *See Porten*, 64 Cal. App. 3d at 828 (sustaining demurrer for failure to plead disclosure to the general public).

Plaintiffs also argue that the alleged unencrypted transmission over WiFi by some App Defendants constituted a disclosure to the public at large, but Plaintiffs do not actually allege that any member of the public at large intercepted such transmissions. Instead, Plaintiffs speculate that the public at large *could have hypothetically* intercepted an unencrypted transmission and thus the alleged unencrypted transmission was a disclosure to the public at large. Speculation, however, is insufficient to support a claim for relief. *See Iqbal*, 556 U.S. at 678 (the "plausibility standard . . . asks for more than a sheer possibility that a defendant has acted unlawfully"). Moreover, the CAC makes clear that several of the apps uploaded the contacts over an encrypted HTTPS protocol, thereby defeating Plaintiffs' own theory. CAC ¶¶ 262, 283, 303.

2. Plaintiffs Do not Allege an Intrusion for a "Highly Offensive" Purpose

Plaintiffs implicitly acknowledge their failure to plead a "highly offensive" use or purpose by arguing that a "highly offensive" use or purpose is not a required element of the claim. Plaintiffs are wrong. As *Folgelstrom* instructs:

> As with the alleged constitutional violation, whether or not plaintiff has sufficiently alleged an intrusion into his private matters, the conduct of which he complains does not meet the standard of "highly offensive." Indeed, **we have found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff's private information which did not also allege that the *use* of plaintiff's information was highly offensive.** However questionable the means employed to obtain plaintiff's address, there is no allegation that Lamps Plus used the address once obtained for an offensive or improper purpose.

Folgelstrom, 195 Cal. App. 4th at 992-93 (emphasis in bold added). Thus, whether the purpose was highly offensive is part and parcel of a common law privacy claim based on a defendant "*obtain[ing] unwanted access to data* about[] the plaintiff." *Id.* Because Plaintiffs do not allege that Defendants invaded a "zone of physical or sensory privacy surrounding," the standard that applies requires a highly offensive purpose. *Id.*

Despite Plaintiffs' hyperbole, they allege only that the App Defendants failed to explain clearly that the apps could access Plaintiffs' contacts before Plaintiffs voluntarily installed the apps on their phones. *See* CAC ¶¶ 19, 24, 31, 32, 355-359. To the extent Plaintiffs now argue that the installation of the apps is the intrusion, Plaintiffs voluntarily installed them, thus negating any intrusion claim. *See Baugh v. CBS, Inc.*, 828 F. Supp. 745, 757 (N.D. Cal. 1993) (noting that "consent is an absolute defense, even if improperly induced" in dismissing intrusion on seclusion claim). To the extent Plaintiffs' claim depends on "unwanted access" to the address data, Plaintiffs must plead a highly offensive purpose.

Plaintiffs attempt to differentiate the circumstances here by citing *Billings v. Atkinson*, but without mentioning that case's most pertinent details. 489 S.W. 2d 858 (Tex. 1973). *Billings* involved allegations that the defendant wiretapped the plaintiff's phone line by installing a device on the "terminal box on the telephone pole behind her house" that would "transmit *conversations* over a standard FM radio." *Id.* at 859 (emphasis added). Plaintiffs here do not allege eavesdropping on private conversations or any remotely similar conduct. Opp. at 26. Instead, Plaintiffs allege that they installed Defendants' apps onto their own phones without full knowledge that the apps could access their contacts. *See* CAC ¶¶ 19, 24, 31, 32, 355-359.

Plaintiffs' allegations are more akin to *Folgelstrom*, which involved the collection of consumers' addresses, than they are to *Billings*. *Folgelstrom* made clear that its ruling was not particular to ZIP codes alone, but address information generally, even when—unlike here—that information was used to send unsolicited advertising materials. *Folgelstrom*, 195 Cal. App. 4th at 992 ("Here, the supposed invasion of privacy essentially consisted of Lamps Plus obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine

commercial behavior."). Judge Koh's ruling on the second motion to dismiss in *In re iPhone Application Litigation* also supports Defendants' position by holding that collection and disclosure of geolocation information from a mobile device "does not constitute an egregious breach of social norms." 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) ("*iPhone II*"). While *iPhone II* involved a California constitutional privacy claim rather than a claim at common law and thus used the "*egregious breach* of social norms" standard, that standard is similar to the "highly offensive" standard applicable here. *See Folgelstrom*, 195 Cal. App. 4th at 993 ("As with the alleged constitutional violation, whether or not plaintiff has sufficiently alleged an intrusion into his private matters, the conduct of which he complains does not meet the standard of 'highly offensive.'").[21]

As Plaintiffs admit that California and Texas law do not differ, the Court should dismiss the common law privacy claims under both states' laws.

3. Plaintiffs Fail to Allege any Harm From the Alleged Privacy Invasion

In addition to failing to establish the required public disclosure or "highly offensive" intrusion required by Texas and California law, both of Plaintiffs' common law privacy claims should be dismissed because Plaintiffs have failed to allege any injury from the alleged invasions of their privacy. *See* Section III.A. Rather than trying to argue any actual injury based on invasion of privacy, they instead ignore the issue completely. For this reason, as well, the Court should dismiss Plaintiffs' invasion of privacy claims.

F. Neither California nor Texas Law Supports a Claim of Conversion Based on Copying Information

Plaintiffs' contention that they can state a claim for conversion by alleging that the App

[21] At no point did the court in *iPhone II* find that the defendants' conduct "was, at most, negligent," as Plaintiffs incorrectly claim. Opp. at 27. To the contrary, the court expressly held: "*Even assuming this information was transmitted without Plaintiffs' knowledge and consent*, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms." *iPhone II*, 844 F. Supp. 2d at 1063 (emphasis added). That decision was also on a motion to dismiss, and thus the court assumed the truth of the factual allegations, including that "Apple began *intentionally* collecting Plaintiffs' precise geographic location and storing that information on the iDevice in order to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States." *Id.* at 1050 (emphasis added). Thus, that court considered the same level of alleged intent and found that it did not support a constitutional privacy violation.

Defendants copied their contacts without alleging the Plaintiffs were deprived of the ability to use the contacts is contrary to both California and Texas law. *See* 5 Witkin, Summary 10th (2005) Torts, § 702, p. 1025 (not all intangible property subject to conversion); Restatement (Second) of Torts § 242 (1965) (same). California law does not recognize a claim of conversion for copying or using information unless doing so completely deprives the plaintiff of the exclusive use of the information. *Kremen v. Cohen*, cited by Plaintiffs, concerned the conversion of a domain name, which is a type of property that is subject to exclusive control. 337 F.3d 1024 (9th Cir. 2003). This is very different than what the CAC alleges—that the App Defendants copied Plaintiffs' contacts but never prevented Plaintiffs from accessing or using the copies on their phones.

Plaintiffs' analogy to a physical address book is inapposite. Though a physical address book can be put in a safe and locked away, stealing the physical book would deprive the owner of its contents. Copying the information in the book, on the other hand, would not. Plaintiffs cite no case holding that mere copying is conversion under California law. *Oakdale Village Group v. Fong* concerned the sale of a promissory note and *eBay, Inc. v. Bidder's Edge, Inc.*, which Defendants discuss in greater detail in the next section, concerned a trespass claim which requires interference, not dispossession. *Oakdale*, 43 Cal. App. 4th 539 (1996); *eBay*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

Judge Gonzalez-Rogers' ruling in *Hernandez* is on point. There, the court held that the plaintiff failed to allege "wrongful disposition of the property right" because he alleged Path had copied (rather than removed) the contacts. *Hernandez*, 2012 WL 5194120, at *7. Plaintiffs still do not allege any Defendant dispossessed them of their contacts. Rather, Plaintiffs have alleged only that Defendants' possession of a copy of the contacts meant that Plaintiffs could not keep Defendants from having a copy of the information. This is simply not a claim for conversion.

Even if Texas law were to apply, its law of conversion is no more permissive. Under Texas law, "intangible property cannot be converted unless the underlying intangible right has been merged into a document that has been converted." *Rehak Creative Servs., Inc. v. Witt*, 404 S.W.3d 716, 734 (Tex. App. 2013). To the extent the U.S. Bankruptcy Court in *Yazoo Pipeline Co., L.P., v. New Concept Energy, Inc.* held otherwise, it did so out of step with Texas law. 459

B.R. 636 (Bankr. S.D. Tex. 2011). Neither Texas state courts nor federal courts in Texas have followed *Yazoo*, and this Court should disregard it as well. *See In re Watts*, 298 F.3d 1077, 1082 (9th Cir. 2002) (noting that federal courts are "bound to follow" state courts of appeal rulings "absent convincing evidence" that the state supreme court would reject them). Instead, this Court should look to the more recent Texas state and federal case law affirming that "Texas law has never recognized a cause of action for conversion of intangible property except in cases where an underlying intangible right has been merged into a document and that document has been converted." *StoneEagle Servs., Inc. v. Gillman*, No. 11-cv-02408-P, 2013 WL 632122, at *9 (N.D. Tex. Feb. 19, 2013) (allowing claim only if intangible information had existed on a taken document) (*citing Express One Intern., Inc. v. Steinbeck*, 53 S.W.3d 895, 901 (Tex. App.-Dallas 2001) *and Carson v. Dynegy, Inc.*, 344 F.3d 446, 456 (5th Cir.2003)); *Rehak*, 404 S.W.3d at 734; *see also Ultraflo Corp. v. Pelican Tank Parts, Inc.*, 823 F. Supp. 2d 578, 587 (S.D. Tex. 2011) ("Texas' conversion law concerns only physical property, not intangible intellectual property rights."). Plaintiffs' other cases are inapposite. *Staton Holdings* concerned a phone number, which is a unique pointer and thus subject to dispossession, and *Hunt* concerned cows that were physically taken. *Staton Holdings, Inc. v. First Data Corp.*, No. 04-CV-2321-P, 2005 WL 1164179 (N.D. Tex. May 11, 2005); *Hunt v. Baldwin*, 68 S.W. 3d 117 (Tex. App. 2001).

G. Plaintiffs Have not Pleaded a Trespass to Chattels Claim

Plaintiffs acknowledge that to plead a claim for trespass to a computer under California law, a plaintiff must allege that the defendant's use of the computer caused injury. *Intel*, 30 Cal. 4th at 1351 (paraphrased by Opp. at 31). Plaintiffs also acknowledge that, like California, Texas requires that plaintiffs allege the App Defendants caused actual damage to their iPhones or that they deprived Plaintiffs of the use of their iPhones for a period of time. Opp. at 30:24-31:1 (citing *Zapata v. Ford Motor Credit Co.*, 615 S.W. 2d 198, 201 (Tex. 1981)).[22] But Plaintiffs then misconstrue two non-precedential decisions in arguing that the unauthorized access and use

[22] *Omnibus Int'l, Inc. v. AT & T, Inc.*, which Plaintiffs cite, supports dismissal. 111 S.W.3d 818 (Tex. App. 2003). There, the plaintiff alleged that AT&T sent unsolicited faxes to plaintiff which deprived the plaintiff of fax machine, paper, and toner. The court granted summary judgment to AT&T, finding that printing of faxes did not deprive plaintiff of the use of its machine "for a substantial period of time." *Id.* at 826.

of a computer without the owner's consent is enough to state a trespass claim. *See id.* (citing *eBay*, 100 F. Supp. 2d at 1071 and *Baugh*, 828 F. Supp. at 756).[23] Even if that were the holding of *eBay* and *Baugh*, the California Supreme Court's subsequent decision in *Intel* sets forth the controlling pleading standard.

In *Intel*, the California Supreme Court made clear that California law requires a plaintiff to allege dispossession of use of the computer for a substantial period of time, or measurable damage to the computer, to state a claim for trespass. *Intel*, 30 Cal. 4th at 1356-57. "Short of dispossession, personal injury, or physical damage (not present here), intermeddling is actionable only if 'the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time.'" *Id.* Moreover, the dispossession of the use of the computer must be so substantial that the plaintiff must be able to estimate the amount of time he was unable to use it. *Id.* "'A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession[.]'" *Id.* (quoting Rest. 2d Torts, § 218, com. i, p. 423). The *Intel* court observed that this requirement was not at odds with *eBay*, where eBay alleged the defendant was bombarding its website with 80,000 to 100,000 unwanted requests from 169 IP addresses *per day*. *eBay*, 100 F. Supp. 2d at 1071.

Plaintiffs' allegations fall short of the pleading requirement established by *Intel* and even the standard applied in *eBay*. At most, Plaintiffs allege the App Defendant's actions momentarily used processing power and battery life of their devices when they accessed Plaintiffs' contacts. But Plaintiffs do not allege any frequency of this access at all and instead allege that they *never noticed* any interference. *See* CAC ¶ 131. Use without damage is not actionable under *Intel*.

Thrifty-Tel, Inc. v. Bezenek, cited by *eBay*, illustrates the difference between use and damage. 46 Cal. App. 4th 1559 (1996). There, repeated automated requests "overburdened the system, denying some subscribers *access* to phones lines." *Id.* at 1564 (emphasis added). In contrast to Plaintiffs' arguments in their briefing, the CAC alleges only that Defendants directed

[23] *Baugh*, in fact, distinguished California cases that had recognized a trespass claim where the defendant exceeded the scope of consent, finding that "[t]hose cases involve defendants whose *intrusion on the land* exceeds the scope of the consent given." *Id.* (emphasis in original). The court went on to reject *Baugh* plaintiff's claim of trespass. *Id.* at 757.

Plaintiffs' iDevices "surreptitiously" to make a transmission without Plaintiffs' express authorization, not that Plaintiffs experienced trouble accessing their contacts or using their phones. CAC ¶ 664. Also, the CAC alleges only that Defendants impaired the value of Plaintiffs' contacts by copying them, not that any function of the iDevices now fails to work.

Plaintiffs also allege no more "use" of their devices' battery, memory, and useful life than the use rejected in *Intel*. *Intel*, 30 Cal. 4th at 1357 (rejecting claim that that email "messages temporarily used some portion of the Intel computers' processors or storage"). Judge Gonzalez-Rogers followed *Intel* in dismissing the trespass claims against *Path*, finding that "any depletion of [a plaintiff's] mobile device's finite resources is rejected as a *de minimis* injury." *Hernandez*, 2012 WL 5194120, at *7. The CAC's trespass claim should be dismissed with prejudice.

H. Plaintiffs Fail to State a Claim Under the Texas Theft Liability Act

Plaintiffs' bald assertion that they have stated a claim under the Texas Theft Liability Act because the App Defendants took Plaintiffs' property without consent must be rejected. As explained in the Motion, the CAC alleges facts showing consent for several defendants. *See* Motion at 3-6. Furthermore, Plaintiffs do not dispute that the CAC fails to allege that the App Defendants intended to or actually withheld Plaintiffs' contacts permanently, for an extended period of time, or that they restored Plaintiffs' access to the contacts only upon payment. Tex. Pen. Code § 31.01(2). Because such allegations are required to state a claim under the Texas Theft Liability Act, Plaintiffs' claim should be dismissed.

I. Opperman Plaintiffs Fail to State a Common Law Misappropriation Claim

Opperman Plaintiffs contend their pleadings establish a common law misappropriation claim because the CAC alleges: (1) that they spent significant time compiling their contacts; (2) that they were "injured" and suffered "commercial damage;" and (3) that the Defendants used their contacts "commercially 'in competition'" with one another and gained a "free ride" by allegedly taking Plaintiffs' contacts rather than purchasing them at fair market value.[24]

[24] Defendants challenge that any data was taken without consent, particularly where, for several apps, Plaintiffs affirmatively chose to have the app "find friends" from their contacts. *See* Motion [Dkt. No. 396] at 3-6, 11 n.5; Twitter, Inc.'s Motion to Dismiss [Dkt. No. 397] at 1-4; Chillingo, Electronic Arts, Rovio and ZeptoLab's Motion to Dismiss [Dkt. No. 393] at 1-4.

These arguments ring hollow for several reasons. First, Opperman Plaintiffs' contention that they suffered "commercial damage" is undermined by the absence from their pleadings of *any* allegations that they ever attempted or intended to sell their contacts and that the App Defendants' conduct prevented them from doing so.[25] *See In re Google Android*, 2013 WL 1283236, at *4 (finding no injury where plaintiffs did not allege they had attempted to sell their data and were foreclosed from doing so by defendants). Not one paragraph in the CAC alleges any attempt or intention by Plaintiffs to sell or market their contacts. *Cf.* CAC ¶¶ 151, 167-71, 680-84. Plaintiffs notably also do not challenge case law holding that no "injury" or "harm" results from claims that personal data has been "devalued" and has "intrinsic, extrinsic, and commercial sales and rental/licensing value." *See, e.g.*, *In re Google Android*, 2013 WL 1283236, at *4; *see also In re TXCO Resources, Inc.*, 475 B.R. 781, 837 (W.D. Tex. Bankr. 2012) (no "commercial damage" established at trial where plaintiff "maintained the possession and use of its data at all times").

Second, Opperman Plaintiffs do not contend they are "in competition" *with* Defendants[26] as required to state a misappropriation claim under Texas law. Rather, they state that the Defendants are using their contact data in competition "with one another." Opp. at 34. Plaintiffs also fail to demonstrate they are commercial competitors who suffered any commercial loss (e.g., loss of customers or business), particularly because they maintained possession of their data. In sum, Plaintiffs' claim for common law misappropriation must be dismissed.

J. Plaintiffs Do not State a Negligence Claim

Plaintiffs' Opposition simply ignores the App Defendants' point with respect to the negligence claim. As set forth in the opening brief, the *only* negligent act Plaintiffs allege is that

[25] Plaintiffs' do not address the inconsistency in their allegation that "[a]ny creation of an address book would take at a minimum several seconds," (CAC ¶ 163) with allegations that significant time was spent on creating an address book with 100-plus contacts. CAC ¶¶ 151, 163, 658. Nor do they point to any detailed allegations to support their alleged "substantial" individual efforts in creating their respective contacts.

[26] While California law does not require the parties to be in direct competition, courts have required plaintiffs to plead that they developed the property at issue through their *commercial* efforts. Plaintiffs fail to describe any such commercial efforts, particularly where they continue to rely on the *personal* and *private* nature of their contact data. *See* Motion at 38.

some of the App Defendants—although Plaintiffs persist in declining to identify which ones—may have transmitted the contents of users' contact folders in unencrypted form or "in the clear." This past conduct, Plaintiffs allege, created the risk that those unencrypted transmissions might have been intercepted. None of Plaintiffs' other allegations against the App Defendants, whether in their complaint or in their Opposition, are allegations of *negligent* conduct, but rather allege—in more than 20 other causes of action—a panoply of *intentional* torts, breaches of contract, and statutory transgressions.

As discussed in Defendants' Motion, however, Plaintiffs' allegation of a past *risk* of harm from the alleged negligence cannot support a cause of action for negligence, because there is no allegation that the alleged risk ever materialized. Nowhere in any of Plaintiffs' hundreds of pages of serial complaints is there a single allegation that anyone's data was in fact intercepted, much less misused as a result of anyone's failure to encrypt it. Nor is there any claim that any App Defendant is continuing to transmit unencrypted data: Plaintiffs allege only past conduct here that ceased more than 18 months ago without anyone's unencrypted personal information being intercepted. Whether some apps' alleged failure to encrypt transmissions *risked* disclosure or not, the CAC does not allege that risk materialized, and thus there was no causation, harm, or damage.

Plaintiffs offer no response to this basic point. Instead, they discuss various of their allegations of *intentional* torts—claims covered in other causes of action—and then point out that *Wine Bottle Recycling LLC v. Niagara Sys.*, No. 12-1924 SC, 2013 WL 5402072, *4 (N.D. Cal. Sept 26, 2013), recognizes certain instances where the economic loss doctrine does not apply to *intentional* torts. This is pure *non sequitur*: The App Defendants have not raised the economic harm doctrine as a defense to Plaintiffs' claims of intentional conduct, but rather to their separate negligence claim, a claim that the doctrine bars. *See id.* (dismissing negligence claims under economic loss doctrine); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 11-2258, 2012 WL 4849054 (S.D. Cal. Oct. 11, 2012) ("Under the economic loss doctrine a plaintiff's tort recovery of economic damages is barred unless such damages are accompanied by some form of physical harm (i.e., personal injury or property damage))"; *see also N. Am. Chem. Co. v. Super. Ct.*, 59 Cal. App. 4th 764, 777 (1997) ("costs of repair and replacement of [a]

defective product" are economic losses, and cannot support a negligence claim).

CONCLUSION

For the reasons stated above and in the App Defendants' opening brief, the App Defendants request that the Court dismiss each claim in the Consolidated Amended Complaint, including their withdrawn RICO and vicarious liability claims, with prejudice.

DATED: January 8, 2014

Respectfully submitted,

FENWICK & WEST LLP

By: */s/ Tyler G. Newby*
Tyler G. Newby (CSB No. 205790)
tnewby@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350

Attorneys for Defendant PATH, INC.

DHILLON & SMITH LLP

By: */s/ Harmeet K. Dhillon*
Harmeet K. Dhillon (#207873)
DHILLON & SMITH LLP
177 Post Street, Suite 700
San Francisco, CA 94108
Tel.: (415) 433-1700
Email: harmeet@dhillonsmith.com

Attorneys for GOWALLA, INC.

Mitchell Silberberg & Knupp LLP

By: */s/ Jeffrey M. Movit*
Jeffrey M. Movit
Mitchell Silberberg & Knupp LLP
12 East 49th Street, 30th Floor
New York, NY 10017
(917) 546-7708 (direct)
(917) 546-7678 (fax)
jmm@msk.com

ATTORNEYS FOR ZEPTOLAB UK LIMITED

DURIE TANGRI LLP

By: */s/ Michael H. Page*
MICHAEL H. PAGE (#154913)
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
Telephone: 415-362-6666
Facsimile: 415-236-6300
mpage@durietangri.com

Attorneys for Defendants
YELP INC. and FOODSPOTTING, INC.

PERKINS COIE, LLP

By: /s/ Timothy L. Alger
Timothy L. Alger
PERKINS COIE, LLP
3150 Porter Dr.
Palo Alto, CA 94304-1212
Telephone: 650.838.4334
Facsimile: 650.838.4350
TAlger@perkinscoie.com

Attorneys for Defendant Twitter, Inc.

COOLEY LLP

By: */s/ Mazda K. Antia*
Mazda K. Antia
Cooley LLP
4401 Eastgate Mall
San Diego, CA 92121-1909
Phone: (858) 550-6000
Fax: (858) 550-6420

Michael G. Rhodes
Matthew D. Brown
101 California Street, 5th Floor
San Francisco, CA 94111
Telephone: (415) 693-2000
Fax: (415) 693-2222

Attorneys for Defendants, INSTAGRAM, LLC and KIK INTERACTIVE, INC.

MORRISON & FOERSTER LLP

By: */s/ David F. McDowell*
David F. McDowell (125806)
Morrison & Foerster LLP
707 Wilshire Boulevard
Los Angeles, CA 90017-3543
Telephone: 213-892-5200
Facsimile: 213-892-5454
Email: DMcDowell@mofo.com

Attorneys for Defendant
FOURSQUARE LABS, INC.

ZWILLGEN LAW LLP

By: */s/ Michele Floyd*
Michele Floyd (SBN 163031)
ZWILLGEN LAW LLP
915 Battery Street, Second Floor, Suite 3
San Francisco, California 94111
Telephone: (415) 590-2340
Facsimile: (415) 590-2335
Michele@zwillgen.com

Marc J. Zwillinger (admitted *pro hac vice*)
marc@zwillgen.com
Jacob A. Sommer (admitted *pro hac vice*)
jake@zwillgen.com
ZWILLGEN PLLC
1705 N St NW
Washington, DC 20036
Telephone: (202) 296-3585
Facsimile: (202) 706-5298

Attorneys for Defendants ELECTRONIC ARTS, INC. AND CHILLINGO LTD.

HOLLAND & KNIGHT LLP

By: */s/ Judith R. Nemsick*
Christopher G. Kelly
Judith R. Nemsick
Holland & Knight LLP
31 West 52nd Street
New York, New York 10019
Tel.: (212) 513-3200
Fax: (212) 385-9010
christopher.kelly@hklaw.com
judith.nemsick@hklaw.com

Shelley G. Hurwitz
HOLLAND & KNIGHT LLP
400 South Hope Street, 8th Floor
Los Angeles, CA 90071
Tel.: (213) 896-2476
shelley.hurwitz@hklaw.com

Attorneys for Defendant ROVIO ENTERTAINMENT LTD. s/h/a ROVIO MOBILE OY

ATTESTATION PURSUANT TO CIVIL LOCAL RULE 5-1(i)

I, Tyler G. Newby, am the ECF User whose identification and password are being used to file this Application Developer Defendants' Reply Brief in Support of Joint Motion to Dismiss Consolidated Amended Class Action Complaint. In compliance with Civil Local Rule 5-1, I hereby attest that all signatories listed above have concurred in this filing.

DATED: January 8, 2014

Respectfully submitted,

FENWICK & WEST LLP

By: */s/ Tyler G. Newby*
Tyler G. Newby (CSB No. 205790)

tnewby@fenwick.com
FENWICK & WEST LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Telephone: 415.875.2300
Facsimile: 415.281.1350

Attorneys for Defendant
PATH, INC.

28603/00403/SF/5457580.21